



Protecting North America's Energy Infrastructure Against Terrorism

Martin Rudner

To cite this article: Martin Rudner (2006) Protecting North America's Energy Infrastructure Against Terrorism, International Journal of Intelligence and CounterIntelligence, 19:3, 424-442, DOI: [10.1080/08850600600656244](https://doi.org/10.1080/08850600600656244)

To link to this article: <http://dx.doi.org/10.1080/08850600600656244>



Published online: 23 Sep 2006.



Submit your article to this journal [↗](#)



Article views: 220



View related articles [↗](#)



Citing articles: 1 View citing articles [↗](#)

MARTIN RUDNER

Protecting North America's Energy Infrastructure Against Terrorism

Global militant Jihadist terrorism has explicitly and directly threatened the international energy industry, and in particular its oil, natural gas, and pipeline sectors. An audio recording, ostensibly from Osama bin Laden in December 2004, declared that “oil prices should be at least \$100 a barrel,” and called upon Jihadist militants to attack oil facilities throughout the Gulf region to prevent the West from getting “cheap” Arab oil.¹ This was the first time that al-Qaeda had openly proclaimed a strategy of harming Western economies by disrupting oil supplies and causing prices to soar. Oil is deemed by militant Jihadists to be the “artery of life to the crusader’s nation,” their term for the United States. According to bin Laden, the strategy being pursued by al-Qaeda aims expressly at “bleeding America to the point of bankruptcy.”²

Four core issues relating to the protection of North America’s energy infrastructure against terrorist threats are:

- (a) the evolving militant Jihadist terrorist threat in the aftermath of the Iraq conflict;
- (b) terrorist tactics and targeting of the energy sector and its infrastructure;
- (c) North American energy integration and its vulnerabilities, criticality, and interdependence with other economic and social sectors; and
- (d) government responses and policy options for critical energy infrastructure protection, public safety, and national resilience.

Dr. Martin Rudner is a Professor at the Norman Paterson School of International Affairs at Carleton University, Ottawa, Canada, and founding Director of the Canadian Centre of Intelligence and Security Studies at Carleton. He is currently a member of the Policy Advisory Panel to Canada’s Arar Commission of Inquiry. Dr. Rudner is a Past President of the Canadian Association for Security and Intelligence Studies.

References made herein to ethno-cultural or religious communities or institutions are not meant to imply that all members of that group are associated with terrorism. Terrorists comprise a small cadre of dedicated, extremist, and highly militant individuals. This study relates to these elements, and their actions.

THE EVOLVING JIHADIST TERRORIST THREAT, POST-IRAQ

The current wave of militant Jihadist terrorism differs from previous manifestations of terrorism by dint of its global purview, networking, and operations.³ Unlike their progenitor, al-Qaeda, the globalized Jihadist militant networks do not have a specific territorial base for their operations, neither do they espouse territorially-defined objectives. Their organizational presence and operational reach extend across geographic borders, regions, and even continents, and now cover Europe, North America, Central, South and Southeast Asia, as well as the Middle East.⁴

Since the overthrow of the Taliban regime in Afghanistan, al-Qaeda and its affiliates have evolved into loosely-structured networks of decentralized subsidiaries, cells (“families”), local auxiliaries or “franchises,” and front organizations.⁵ Militant Jihadists have demonstrated remarkable adaptability by way of transforming themselves into an eclectic array of groups, cells, and motivated individuals that do not require a fixed headquarters, but engage in recruitment and fund-raising, while acquiring training materials, weapons know-how, and targeting guidance through the Internet.⁶ As a high-ranking British intelligence official observed: “Al-Qaeda has split like a piece of mercury into different groups in different countries.”⁷ Yet, even as they evolve and adapt, al-Qaeda, its affiliates, and Jihadist partners have remained committed to a shared strategic outlook, to mutual support for tactical synergy, and to mobilizing combatants to fight wherever the Jihadist cause invokes the defense of Islam by the taking of offensive action.

Targeting Civilians

The U.S.-led invasion of Iraq and overthrow of the regime of Saddam Hussein has resulted in two separate and distinct insurgencies, one waged by a Ba’athist, nationalist resistance, and the other by “al-Qaeda Between the Two Rivers”—the Jihadist nomenclature for Mesopotamia/Iraq. Whereas the Ba’athist nationalists attacked the foreign presence, al-Qaeda mounted a deliberate campaign of terror (“martyrdom operations”) targeting primarily Iraqi civilians, officials, police, and national infrastructure. These assaults were aimed at decimating the despised Shi’a majority population (“the lurking snake, the crafty and malicious

scorpion”) and overthrowing the emergent elected government, which would in turn force an American and Coalition withdrawal and culminate in a decisive victory for Jihadism in the “Arab heartland.”⁸ For al-Qaeda, “the land of Mesopotamia” had replaced Afghanistan as the bastion and “decisive” battleground from whence to wage a relentless Jihad against the perceived enemies of extremist Islam: domestic, regional, and global.⁹

Outsiders Arrive

A particularly worrisome aspect of the al-Qaeda assault on Iraq is the large number of *mujahiddin* (holy warriors) from other Middle Eastern countries and from Muslim communities in Europe who have been recruited to fight alongside local combatants. In early 2005 French intelligence officials estimated that some 2,000–3,000 foreign fighters were then in Iraq.¹⁰ Others claimed the number could be considerably greater, though the al-Qaeda leadership admitted in 2004 that “(t)heir numbers continue to be negligible as compared to the enormity of the expected battle.”¹¹ Most foreign recruits in Iraq have come from Saudi Arabia, Syria, Egypt, Jordan, Yemen, and Kuwait.¹² In Europe, the recruitment of foreign *mujahiddin* for Iraq has extended to Britain, France, Germany, Spain, Italy, and Norway, and now occurs in other countries as well, among them Belgium and Switzerland.¹³ Certainly, the fear is that when these foreign *mujahiddin* return to their home countries they will become agents for the promotion of extremist Islamic doctrine, a repeat of the experiences of Afghanistan, Bosnia, Chechnya, and Kashmir. European governments seem to be especially concerned that Iraq’s *mujahiddin* would also bring with them combat experience in fighting against the “Best of the West,” along with an energized dedication to Jihadist activism at home and abroad.¹⁴

TERRORIST TACTICS AND TARGETS

Militant Jihadism considers itself engaged in a sacralized conflict of global proportions as between *Dar ul-Islam*, the abode of Islam, which they deem divinely perfect and righteous, and the *Dar ul-Harb*, the domain of the unfaithful, characterized by corrupt values, moral chaos, and heresy. The overarching goal of the militant Jihad is to (re-) establish a pan-Islamic Caliphate, a *Dar ul-Islam* spanning the world. Al-Qaeda foresees that this will occur through the forced Islamization of the United States of America, which in turn would bring all other countries into a worldwide Islamic realm. Terrorism is deemed by Jihadists to be both a legitimate defensive tactic against perceived enemies of Islam, and a justifiable offensive strategy to attack and destroy erstwhile infidels and “apostate” Muslim states.¹⁵

Ruthless Versatility

Al-Qaeda and its affiliated Jihadist militants have demonstrated a high degree of flexibility and inventiveness in selecting targets and exploiting new vulnerabilities. Their assaults are characterized by stealth, surprise, and ruthless ferocity. According to a recent report by the Norwegian Defence Research Establishment, *Jihad in Europe*, al-Qaeda and its affiliates attempted or perpetrated some thirty “spectacular” attacks against targets in or from Europe between 11 September 2001 and the end of 2003.¹⁶ Recent terrorist plots and attacks have targeted economic assets, notably urban transit systems, energy infrastructure, civil aviation, tourism facilities, and commerce. Mass casualties and political shock were compounded by the destruction of physical assets, capital losses, market upheaval, and business disruption.¹⁷ The ensuing damage to national and global economic systems has been massive, costly, and long-lasting. Indeed, the mere threat of terrorist assault can impose costly protective measures on prospective targets.

Targeting Oil and Power

Up to the time of writing no database on terrorist targeting or incidents involving the energy sector, as such, is publicly available. The global database on terrorist incidents and organizations, sponsored by the U.S. National Memorial Institute for the Prevention of Terrorism (MIPT), does not relate to the energy sector as a specific target area. To obtain a comprehensive perspective on international experiences in this sensitive and vital domain is therefore difficult, if not impossible. Nevertheless, the Iraqi insurgency has demonstrated the particular vulnerability of energy infrastructure to terror attacks.

Insurgents have targeted Iraq's oil sector in a sustained and orchestrated effort to prevent the emergent government from exploiting this valuable natural resource, to undermine confidence and support for the elected administration, and to derail its program of economic rehabilitation.¹⁸ Certainly, oil exports proved to be exceptionally vulnerable because oil can be transported out of Iraq through only two main corridors: via Basra by sea, and by pipeline from Kirkuk to Ceyhan in Turkey. The initial projection was that oil production and exports would offset the costs of the Iraq war and post-war reconstruction. Even though the protection of oil installations became a top priority for the Allies' Coalition Provisional Authority, with some 14,000 security personnel being dedicated specifically to that task, insurgent attacks on Iraq's energy infrastructure have continued incessantly. The assault has targeted pipelines, trunk lines, refineries, oil wells, storage tanks, oil company workers and managers, loading terminals, and other installations. These attacks have caused severe damage to the Iraqi economy,

curtailing production, cutting local supplies, and disrupting exports.¹⁹ Since oil contributes the bulk of the emergent national government’s revenue, reduced exports have resulted in acute budgetary shortfalls which in turn retard progress on economic and social reconstruction.

The terrorist assault on Iraq’s energy infrastructure has also targeted the electric power system.²⁰ Attacks have been directed at electricity generating plants, their fuel supplies (oil), and the power grid. The resulting destruction has caused frequent and recurrent power outages in all parts of the country. Occasionally, the entire national electric grid has been shut down. The harm inflicted on Iraq’s oil and power infrastructure demonstrates clearly the potential for al-Qaeda to inflict massive and far-reaching damage on targeted countries by attacking the energy sinews of their economies. By December 2004, al-Qaeda was calling on militants throughout wider Arabia to target petroleum installations in their Jihad against the infidels and their local allies.²¹

With crude oil in short supply internationally, and prices reaching historic peaks, any significant loss of production could cause massive dislocations to the industrial economies of Asia, Europe, and North America, and to Middle East and other developing countries as well. Attacks on petroleum supplies anywhere in the world have the potential to harm the U.S. directly, given its energy dependency, while also wreaking havoc with other countries’ economies through even higher oil prices.

Matrix 1. Al-Qaeda’s 20-Year Strategic Plan.

Stage	Strategic Aim	Timeline	Tactical Objectives
1	“Awakening”	11 September 2001	Provoke U.S. attack on Muslims, galvanize Jihadism
2	“Opening Eyes”	2003–2006	Force West on defensive
3	“Arising and Standing Up”	2007–2010	Assaults on Turkey and Israel
4	“Downfall of Apostate Muslim regimes”	2010–2013	Saudi Arabia, Jordan, oil producers
5	“Declaration of Caliphate”	2013–2016	Mobilization of Muslim forces
6	“Total Confrontation”	2013–2020	Total war on “non-believers”
7	“Definitive Victory”	2020	A Muslim world

Al-Qaeda's leadership is obviously pursuing a seven-stage, twenty-year grand strategy for the Jihadist struggle for global supremacy, aimed at achieving a "definitive victory" by 2020.²² This "plan," which is said to represent the strategic guidelines for a successor generation al-Qaeda leadership, is exemplified by Abu Musab al-Zarqawi, leader of al-Qaeda "Between the Two Rivers" (i.e., Iraq). Each stage has a strategic aim, an indicative timeline, and tactical objectives, as set out in Matrix 1.

NORTH AMERICAN ENERGY INTEGRATION, VULNERABILITIES, CRITICALITY

The energy sector represents a vital component of the economies of Canada, the United States, Mexico, and Caribbean countries like Trinidad and Tobago, and makes a substantial contribution to national income, employment, economic activity, exports, and growth. Energy production has risen substantially since 1970 throughout the Americas, and is expected to continue growing through 2020. But North America's share of the world's energy production has fallen substantially over recent decades, and this is expected to continue (to about 21 percent) through 2020.²³ North America's energy economy is closely integrated continentally, with connectivity maintained by pipeline networks, electricity grids, and extensive commercial interactions among operators in the industry. Continental energy integration is further sustained by regional trading arrangements, such as the North American Free Trade Area (NAFTA).

Northern North America

Canada's energy sector involves the production and refining of petroleum, natural gas, coal mining, and electricity generation from hydro, oil, gas, coal, and nuclear power plants.²⁴ Fossil fuels are produced, primarily, from Canada's Western Sedimentary Basin, and from offshore oil and natural gas fields on the east coast. The nuclear power industry, fueled by domestic uranium, operates twenty-two Candu reactors in Canada. Coal, mined domestically, is the primary fuel for electricity generation in a number of provinces. Oil and gas extraction and related support activities contributed 4.2 percent of Canada's Gross Domestic Product (GDP) in 2003, the latest year for which data is available.²⁵ In previous years, the energy sector as a whole contributed over 7 percent of GDP, and accounted for annual investment of some C\$24 billion (US\$15.6 billion, approximately).²⁶ Certainly, the oil price surge of 2004–2005 will have greatly increased this contribution.

Canada in 2002 exported more than half its total production of primary energy, including petroleum, natural gas, and electricity, in terms of oil

equivalents.²⁷ Exports of energy products totaled C\$60.5 billion in 2003 (US\$39 billion, approximately), or about 15 percent of Canadian merchandise exports.²⁸ Of these energy sector exports, natural gas contributed C\$26 billion, petroleum C\$20 billion, and other energy products C\$13 billion. Canada, an energy exporter, is closely coupled through infrastructure links to an integrated North American energy market.²⁹ Canada sends over 99 percent of its crude oil exports to the United States, and the country is one of the most important sources of U.S. oil imports. Some 56 percent of Canada's natural gas production is exported to the U.S. As for electricity, in 2003 Canada exported 29.3 Bkwh to the United States, while importing 23.6 Bkwh from the U.S. In recent years, Canadian electricity exports to the U.S. have decreased while imports have increased, because investment in Canadian generating capacity has lagged behind a growing domestic demand.³⁰

Southern North America and the Islands

Mexico, for its part, ranks as the world's fifth-largest oil producing country, after Saudi Arabia, Russia, the United States, and Iran.³¹ The Bay of Campeche is the mainstay of that country's oil production. Mexico exports about half its 3.8 million barrels per day oil output, mostly to the United States. This has made Mexico the third largest supplier of oil to the U.S., behind only Canada and Saudi Arabia. Although the country is home to the Western Hemisphere's sixth-largest natural gas reserves, domestic demand has far outpaced Mexican production over the last decade, leaving a deficit that had to be filled by imports from the United States.

Trinidad and Tobago is the largest Caribbean producer of oil and natural gas.³² These hydrocarbons contributed over 40 percent of the country's GDP in 2004, a figure that increased along with subsequent rises in energy prices. In 2004, Trinidad and Tobago produced 165,000 barrels of oil per day, mainly for export to the United States. The island country is also the largest supplier of liquified natural gas (LNG) to the United States, supplying nearly 75 percent of U.S. LNG imports.

The Thirsty Giant

The United States, the world's largest energy producer and consumer of commercial energy, is also the largest net importer.³³ Over 43 percent of the total U.S. oil refining capacity is concentrated along the Gulf coasts of Texas and Louisiana.³⁴ Overall, oil provides about 40 percent of the total U.S. primary energy requirements; natural gas for some 24 percent, and coal for 23 percent. Nearly 58 percent of the U.S. demand for oil in

2004 was met by imports. The main sources of supply, in order of magnitude, were Canada, Mexico, Saudi Arabia, Venezuela, and Nigeria. About a quarter of U.S. natural gas consumption in 2004 was met by imports, 80 percent of which came from Canada. Mexico is a net importer of natural gas from the United States.

Extensive networks of pipelines and power grids transmit oil, natural gas, and electricity from points of production to consumers and user industries across Canada, the United States, and Mexico. The vast U.S. electricity grid consists of nearly 20,000 transmission lines and over 14,000 substations.³⁵ Canada's system of transmission pipelines extends for 80,000 kilometers and is connected to 345,000 kilometers of local distribution pipelines. Mexico has 5,652 miles of natural gas pipelines. Trinidad and Tobago also has an extensive pipeline network linking offshore oil and gas fields to onshore landing points. As of 2004, the U.S. natural gas pipeline network covered some 226 gas pipeline systems with more than 306,000 miles of pipeline. Expansion of the North American pipeline network over recent decades has been driven in large part by the growing U.S. demand for Canadian natural gas. The U.S. and Canadian natural gas grids have become closely interconnected, with Canadian natural gas supplying an increasing share of the total U.S. demand. This is especially true for certain U.S. regions, such as the Northeast, Midwest, the Pacific Northwest, and California, which depend on Canadian natural gas for a significant proportion of their supply.

In March 2001, the energy ministers of Canada, Mexico, and the United States met to discuss a common energy strategy for the three countries, including an integration of their power grids. Considerable reciprocity already exists between the electric power sectors of Canada and the U.S. Canada exports electricity from Quebec and New Brunswick to New England and New York, with smaller volumes going from British Columbia and Manitoba to Washington State, Minnesota, California, and Oregon, while the U.S. exports electricity to Ontario and other Canadian power-deficit regions. By way of contrast, electric power connectivity between Mexico and the United States is much more limited. Only three transmission lines crossed the Mexico–U.S. border at the start of 2004, so that inadequate infrastructure remained a major constraint on wider electrical sector integration.

The Vulnerability Factor

Various elements of the energy infrastructure have their own particular vulnerability to terrorist attack, and their own criticality in terms of interdependency and ramifications for other sectors of the economy and society. Oil and natural gas wells may seem to be vulnerable individually,

but their being scattered across the landscape diminishes their overall exposure as a sector. Refineries, natural gas processing plants, electricity generating stations, control systems, compressor stations, gate stations, and storage facilities constitute singularly high-value potential targets, but they are typically well-protected to reduce their vulnerability, though offshore production platforms may be vulnerable to assault from sea or air. Pipelines and transmission systems would be inherently difficult to protect throughout and are especially vulnerable to sabotage, but the risks may be mitigated by protective measures and system redundancy.³⁶ Alas, gaps in protection represent vulnerabilities to determined terrorists.

The geographic concentration of certain energy assets, and most notably oil refineries, gas processing plants, offshore platforms, loading platforms, pipeline networks, and power grids, can render this infrastructure more vulnerable to large-scale disruption.³⁷ The electric power grid and oil/natural gas pipelines have quite different geographic densities: the spread of electric power is far more uniform than that of oil and natural gas, exposing them to quite different risks.³⁸ But a very high density of transmission lines exists around the middle of Ohio, close to the fulcrum of the August 2003 blackout.³⁹ To be sure, the density of energy assets in certain geographic areas, like the refineries on the United States's Gulf Coast, reflects their locational advantages economically. But the confluence of energy infrastructure offers not only multiple high-value targets for terrorists, and may facilitate the spread of the cascading consequential impact of any attack far beyond the targeted site.

Measuring Vulnerability

Assessments of threats, vulnerability, and criticality for North America's energy infrastructure may be plotted on a Critical Energy Infrastructure Protection (CEIP) Terrorism Vulnerability Matrix. Matrix 2 provides general estimates of the various degrees of threat, vulnerability, and criticality for each of the major sectoral and structural components of North America's energy industry. A detailed application of the CEIP Terrorism Vulnerability Matrix may be helpful for analyzing the CEIP requirements and for identifying specific operational priorities. In principle, those threat assessments, vulnerabilities, and criticality elements estimated to be "H" (high) warrant more urgent policy and operational responses than those rated "L" (low).

The indicators of threat and vulnerability appear to highlight the relatively high level of terrorism risk pertaining to trunk pipelines, compressors and gate stations, control facilities, offshore platforms, and the electric grid. Oil refineries and natural gas processing plants also constitute relatively high-risk infrastructure, but their vulnerability may

Matrix 2. Critical Energy Infrastructure Protection—Terrorism Vulnerability Matrix.

Function	Installation	Assessment		
		Threat	Vulnerability	Criticality
<u>Extraction</u>				
	Wells	L	L	M
	Offshore Platforms	M	H	H
	Mines	L	L	L
<u>Processing</u>				
	Refineries	M	H	H
	Processing Plants	M	H	H
	Generating Stations	L	L	H
	Control Systems	H	H	H
<u>Storage</u>				
	Tank Farms	L	M	M
	Transformers	L	L	L
<u>Transport</u>				
	Pipelines—Trunk	H	H	H
	Pipelines—Distribution	M	M	M
	Transmission Grid	M	H	H
	Loading Platforms	L	L	M
	Compressor Stations	H	H	H
	Gate Stations	H	H	H
	Tanker Trucks	L	M	L
	Rail Cars	L	M	L

Key: H: High; M: Medium; L: Low.

be offset by appropriate fortification measures. Particular risks accrue to the nuclear energy subsector, including extraction, processing, transport, power generation and storage, in view of al-Qaeda’s known quest to acquire chemical, biological, radiological, and nuclear (CBRN) weaponry capability. But these risks are mitigated in good measure by the stringent regulatory controls applied to nuclear facilities. Other elements of energy infrastructure seem to be less at risk as individual installations.

Effects of Vulnerability

North America’s energy infrastructure possesses a high degree of criticality for the national economies, for consumers and user industries, and for the

public well-being. Oil, natural gas, and electricity production are operating at or near capacity, with little if any spare capacity readily available. A sudden loss of production capacity because of terrorist attacks would cause prices to spike. This could result in far-reaching dislocation and hardship, over and above any casualties and physical damage.

Energy infrastructure exhibits differing levels of criticality based on the relative contribution of particular assets, oil, natural gas and electricity, to overall supplies, and the substitutability of their output. Yet, the criticality of energy infrastructure extends beyond just the economy. The consequential effects of a terror attack on North America's energy infrastructure would likely reverberate on public confidence in the ability of government to protect core national interests, and on neighboring countries' willingness to depend on partners for their national security generally, and for energy sourcing in particular. In that sense, the ultimate measure of criticality, especially for Canada, Mexico, and the Caribbean, would be the very sustainability of North American energy integration in the event of a terror attack on a critical infrastructure component. Thus, the mere risk of terrorist activities taking place in or through a country like Canada can suffice to impel other friendly governments, including the United States, to tighten controls on cross-border movements of persons and goods. This could cost Canadians dearly.

RESPONDING TO THREATS TO CRITICAL ENERGY INFRASTRUCTURE

Faced with the asymmetric threat to national security and public safety, governments have assigned high priority to the protection of North America against terrorist attacks. But the policy framework for Critical Energy Infrastructure Protection in Canada and the United States is rendered especially complex by virtue of private sector ownership of most energy assets, coupled with divided federal-state/province jurisdiction over this domain. In Trinidad and Tobago, a unitary system of government exercises jurisdiction over an energy industry that is largely foreign-owned. Mexico presents a somewhat different situation because federal monopolies operate the national energy infrastructure: *Petróleos Mexicanos* (Pemex) in the production, refining, and marketing of petroleum and natural gas, and the *Comisión Federal de Electricidad* (CFE) in electric power generation. For Canada and the United States, at least, their respective architecture for CEIP policy can therefore involve intricate issues regarding administrative, regulatory, intelligence, and law enforcement responsibilities at the federal and local state/provincial and municipal levels, and those between public and private sector stakeholders. In all countries, CEIP invokes a policy conundrum over jurisdiction, powers, timing, and operations:

- a. *Jurisdiction*: the structure of governmental authority over CEIP, whether centralized or decentralized, federally or departmentally;
- b. *Powers*: the mandates allocated among the various governmental institutions having responsibility for CEIP, whether administrative and policy management, or regulatory, or intelligence collection and assessment, or emergency planning, or law enforcement;
- c. *Timing*: the license for government interventions for CEIP protection, whether proactive though preemptive defense, security intelligence and law enforcement, or reactive on the part of first-responders or consequence management;
- d. *Operations*: the range of activities authorized by government for CEIP protection, which could include command and control over energy assets, security coordination, early warning systems, information sharing, intelligence interventions, law enforcement, training and exercises, and/or protective security.

The recent reforms of the United States Intelligence Community assigned responsibility for the protection of the country's critical energy infrastructure, at the federal level, to the Department of Homeland Security, and for nuclear power facilities to the Department of Energy. The U.S. Department of Defense has taken upon itself an expanded role in ensuring an "active, layered" approach to homeland defense and civil support against terrorism.⁴⁰ Yet, this reformed architecture for U.S. national security remains essentially defensive, being geared to defense, detection, and disruption of identified threats to particular critical (energy) infrastructure assets, coupled with consequence management.⁴¹ Thus, the Department of Homeland Security embarked on a National Planning Scenarios exercise, identifying plausible terrorist targets and their likely toll, in terms of casualties and economic damage.⁴² This exercise, which is still classified, reportedly reflects the Department's current approach to risk-based planning. It seeks to identify the most plausible and devastating risks, consistent with known terrorist capabilities and tradecraft, and then design appropriate responses to deal with these.⁴³ Policy remains focused on macro-level homeland security, as distinct from the micro-level protective security of a particular infrastructure, with emphasis directed at risk management, probabilities assessment, and damage mitigation. The burden is placed on private and public sector proprietors to minimize the vulnerabilities of their own productive assets.

The protection of Canada's critical national infrastructure against terrorist threats is a priority concern of the country's National Security Policy.⁴⁴ Responsibility for "leadership" in designing a Critical Infrastructure Protection Strategy was vested in the newly formed Department of Public Safety and Emergency Preparedness Canada (PSEPC).⁴⁵ But, in the Canadian system, jurisdiction over the energy industry is a shared responsibility between different levels of government and between the public and private sectors. Security, law enforcement, administration,

regulatory authority, and emergency preparedness are similarly divided among departments and levels of government. As a result, policy and regulatory authority over the protection of the critical energy infrastructure is decentralized among several pertinent department and agencies of the government of Canada, the provinces and territories, municipalities, and owners and operators of particular assets.

Canada's federal, provincial, and territorial ministers responsible for public safety and emergency management met in early 2005 and agreed to develop a work plan for a national Critical Infrastructure Protection Strategy. Meanwhile, line departments remain primarily responsible for policies within their respective precincts and within federal areas of jurisdiction, that is, Transport Canada for transportation security; Natural Resources Canada for critical energy infrastructure protection. Canadian defense planners participated with their U.S. counterparts in a Bi-National Planning Group to develop coordinated military planning to support civil authorities in the event of a terrorist attack on North America. Nevertheless, weaknesses and gaps remain in Canada's policy framework for dealing with threats to its critical national infrastructure.⁴⁶ The Canadian government does not yet have in place a centralized clearinghouse for information pertaining to critical energy infrastructure protection for its own departments and agencies, or for sharing with other jurisdictions.

In Mexico, and in Trinidad and Tobago, national governments exercise exclusive jurisdiction over their respective oil, natural gas, and electricity sectors. Neither has seen fit to establish a dedicated department or agency responsible for protecting critical national infrastructure. In both countries, the protection of energy industry assets remains vested in line ministries and security and law enforcement authorities, and with private owners, for their part.

Private and public sector owner/operators of various elements of the critical energy infrastructure have established their own organizational mechanisms for information sharing and cooperation in the management and mitigation of threats. Thus, the electric power industry has set up ten regional "reliability councils" across the U.S. and Canada, capped by a North American Electric Reliability Council (NERC) for the setting and enforcing of reliability and performance standards. Similar mechanisms exist for other energy sectors, including oil and natural gas producers and pipeline operators. In the United States, the various industrial groups are brought together into a consultative arrangement with government through dedicated Information Sharing and Analysis Centers (ISACs) for the energy industry and electricity sector, among others. Whereas industrial self-regulation for the energy sector may provide standards for the assurance of systems' adequacy and performance, rarely, if ever, are these

self-regulatory standards designed to respond to particular, potentially devastating threats.

CEIP Policy across the various North American jurisdictions thus remains essentially defensive, emphasizing emergency preparedness, assurance, and mitigation management. A defensive posture is procedurally passive and tactical, rather than strategic and proactive. Harnessing critical (energy) infrastructure protection to a centralized, macro-level framework for preparedness planning inhibits the taking of calibrated initiatives to develop countermeasures for dealing with asymmetric threats. This passive, defensive orientation has tended to impede the formation of partnerships—domestically with subnational jurisdictions and with the private sector, as well as internationally. Ultimately, a defensive, passive, tactical approach to CEIP Policy will, in effect, constrain the building of national capacity to address the contemporary threat environment.⁴⁷

A STRATEGIC APPROACH TO INTELLIGENCE-LED CEIP

In his 2005 article, “Intelligence and Homeland Defense,” in *Transforming U.S. Intelligence*, edited by Jennifer Sims and Burton Gerber, Henry Crumpton makes a case for integrating security intelligence with homeland security in order to generate synergy for a more proactive defense of the realm.⁴⁸ Whether his prescriptions for institutional reform are accepted or not, the notion of fusion between security intelligence and critical infrastructure protection merits attention. Indeed, some countries, including Canada, already mandate their security intelligence services and law enforcement agencies to collaborate with public security and line departments, at least formally. Yet, fusion and operational synergy remain beyond the pale. The fulfillment of governments’ commitments to public safety and homeland protection would surely call for a proactive, calibrated, intelligence-led strategy for dealing with threats to critical national infrastructure, including and especially energy.

A proactive, cooperative approach to CEIP by governments would, moreover, meet emergent legal standards applicable to democratic governance.⁴⁹ With governmental immunities being whittled away by the courts, proactive partnering could avert any risk of possible public litigation for compensation due to governmental negligence for injuries or damages sustained in a prospective terror attack. Information sharing between governments and industry stakeholders, as appropriate, would also meet legal requirements for the fulfillment of fiduciary duties to share beneficial information for the advantage of others with whom there are special relationships.

In intelligence, as in war, a good defense is predicated on a robust offense. The architecture for a proactive, intelligence-led strategy for critical (energy)

infrastructure protection would necessarily focus on both micro-level and macro-level security. A robust offense should defend against terrorist threats to particular targets, in addition to preplanning for homeland resilience. A proactive, intelligence-led approach to critical infrastructure protection would demonstrate the following attributes:

- The strategic goal would be to identify, prevent, and defeat threats to critical infrastructure and public safety.
- Tactical doctrine would impel intelligence-led law enforcement toward the calibrated systematic collection, analysis, and reporting on threats to critical national infrastructure.
- The precept of Security Intelligence would undergo a cultural shift from a traditional reticence, based on “need to know,” to a recognition of the “need to share” pertinent information.
- Private sector owners/operators of critical infrastructure assets would be expected to share their own assessments of vulnerabilities and threats with security authorities, on a classified basis.
- Security intelligence assessments of threats to critical (energy) infrastructure also would be disseminated to security-cleared personnel in targeted private sector facilities.

Based on these attributes, an intelligence-led approach to critical (energy) infrastructure protection would deploy the intelligence capabilities to detect and penetrate terrorist elements that threaten public safety and target infrastructure from within the country or abroad. Sophisticated data-mining technologies and network analysis techniques would be utilized to discern subtle insights and threatening trends in the vast storehouses of Intelligence Community databases. Operational partnerships between intelligence and law enforcement communities, involving all intelligence disciplines and international partners, would enable a fast, agile tracking of risks. An integrated, all-source analytical capability would be expected to feed actionable intelligence assessments to operational elements. A counterintelligence and protective security capability is vital to prevent destructive adversaries from penetrating the national security system.

An often neglected aspect of innovations to intelligence and security architecture is their implicit training prerequisites. To be effective, a shift to an intelligence-led strategy for critical national infrastructure protection would entail the introduction of a comprehensive training program for intelligence officers, analysts, and policy managers, to equip them with the requisite specialized knowledge and skills to understand the threats, vulnerabilities, and criticality associated with specific industrial sectors, as well as their organizational attributes and needs. Likewise, first responders should be provided appropriate training and exercises to equip them to deal with probable scenarios.

Private sector owner/operators would incur reciprocal obligations as part of the shift to a new intelligence-led approach to the protection of critical energy infrastructure. The new security intelligence culture imparts reciprocity as regards duties, as well as shared advantages. Private sector owner/operators should be expected to embed security into the design of critical infrastructure facilities, to decrease vulnerabilities, and mitigate consequential damage. Standards for protective security and resilience planning should be set and enforced for all key assets of the critical national infrastructure. Information about vulnerabilities and threats must be shared, reciprocally, and in a protected manner, with security and intelligence services.

The thrust of a new approach would be to transform the paradigm for CEIP policy from risk management to counterterrorism. Lessons learned from the evolution of al-Qaeda in Iraq indicate that any gaps in protective security represent vulnerabilities to determined terrorists. Yet, democratic, open societies will always experience gaps in protective security. Therefore, policy managers must ensure that the cost to adversaries of trying to exploit these vulnerabilities is high, their prospects of success minimal, the potential consequential damages mitigated, and that industry and society are prepared for resilience.

REFERENCES

- ¹ *Al-Quds al-Arabi* [London], 17 December 2004; see also Mordechai Abir, "The Al-Qaeda Threat to Saudi Arabia's Oil Sector," Jerusalem Center for Public Affairs, *Jerusalem Issue Brief*, Vol. 4, No. 13, 28 December 2004, <http://www.jcpa.org/brief/brief004-13.htm>.
- ² "Full Transcript of bin Laden's Speech," *AlJazeera.net*, 30 October 2004, <http://english.aljazeera.net/NR/exeres/79C6AF22-98FB-4A1C-B21F-2BC36E87F61F.htm>.
- ³ Neil Smelser and Faith Mitchell, eds. *Terrorism. Perspectives from the Behavioral and Social Sciences*. National Research Council of the National Academies (Washington, DC: The Academies Press, 2002); Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004); Malise Ruthven, *A Fury for God: The Islamist Attack on America* (London: Granata, 2002); Walter Laqueur, *Voices of Terror: Manifestos, Writings and Manuals of Al Qaeda, Hamas, and Other Terrorists from Around the World and Throughout the Ages* (New York: Reed Press, 2004).
- ⁴ Petter Nesser, *Jihad in Europe—A Survey of the Motivations for Sunni Islamist Terrorism in Post-millennium Europe*, FFI Report FFI/RAPPORT-2004/01/1146 (Oslo: Norwegian Institute for Defense Research, 2004), esp. pp. 18–27; Jason Burke, *Al-Qaeda: Casting a Shadow of Terror* (New York: I.B. Tauris, 2003); Jane Corbin, *Al-Qaeda: In Search of the Terror Network that Threatens the World* (New York: Thunder's Mouth Press, 2002); Yoram

Schweitzer, *The Globalization of Terror: The Challenge of Al-Qaeda and the Response of the International Community* (New Brunswick, NJ: Transaction Publishers, 2003); Anonymous (Michael Scheuer), *Imperial Hubris: Why the West Is Losing the War on Terror* (Washington, DC: Brassey's, 2004).

- ⁵ *Mapping the Global Future*, Report of the National Intelligence Council's 2020 Project (Washington, DC: U.S. Government Printing Office, December, 2004), p. 94.
- ⁶ National Intelligence Council, *Mapping the Global Future*; Dana Priest, "Iraq New Terror Breeding Ground," *The Washington Post*, 13 January 2005.
- ⁷ Cited in Robin Gedy, "Saudis Put on a Show for Terror Summit," *Daily Telegraph* [London], 7 February 2005.
- ⁸ "To the Proudest of Persons and Leaders... To the Men on the Mountain Tops, to the Hawks of Glory, to the Lions of the Shara..." letter attributed to Abu Musab al-Zarqawi, leader of the terrorist group *Tawhid wal Jihad*, later renamed Al-Qaeda Between the Two Rivers (Iraq), *Pt. 4.—The Work Plan*. This letter was reportedly seized from a captured operative in Iraq and released by U.S. officials in 2004. <http://www.cpa-iraq.org/transcripts/20040212-zarqawi-full.html>
- ⁹ "To the Proudest of Persons and Leaders..." preamble. See also Richard Beeston, "The Terror, The Terror," *The Spectator* [London], 23 September 2004; Craig Whitlock, "Grisly Path to Power in Iraq's Insurgency," *The Washington Post*, 27 September 2004.
- ¹⁰ Elaine Sciolino, "France Seizes 11 Accused of Plotting Iraq Attacks," *The New York Times*, 27 January 2005.
- ¹¹ "To the Proudest of Persons and Leaders..." *Part 2. E-The Immigrant Mujahidin*.
- ¹² "Saudi Scholars: Support Iraqi Fighters," *Al-Jazeera*, 6 November 2004. <http://english.aljazeera.net/NR/exeres/DF6DD7BA-3B43-45A0-94EA-6D7B0FICCEEB.htm>
- ¹³ Craig Smith and Don Van Natta, Jr., "Officials Fear Iraq's Lure for Muslims in Europe," *The New York Times*, 23 October 2004.
- ¹⁴ Peter Bergen and Alex Reynolds, "Blowback Revisited," *Foreign Affairs*, Vol. 84, No. 6, November–December, 2005, pp. 2–6.
- ¹⁵ Malise Ruthven, *A Fury for God*, Chapters 2 and 3.
- ¹⁶ Petter Nesser, *Jihad in Europe*, pp. 79 *et seq.* Of this number, 14 were impending, interrupted conspiracies; 18 were thwarted threats; 4 were "exported" attacks launched from Europe against targets elsewhere; three were actual attacks in Europe itself.
- ¹⁷ See the terrorism incident database compiled by the U.S. National Memorial Institute for the Prevention of Terrorism (MIPT) at <http://db.mipt.org/Home.jsp>. See also Petter Nesser, *Jihad in Europe*, p. 89.
- ¹⁸ "Attacks Cripple Iraq Oil Exports," BBC News, 15 June 2004: <http://newsvote.bbc.co.uk/pagetools/print/news.bbc.co.uk>

- ¹⁹ "Attacks Hit Iraq Oil Exports," *Al-Jazeera*, 15 June 2004: <http://english.aljazeera.net/NR/exeres/361AE282-007E-4A0E-922E-C88443E2EAFf.htm>; Richard Sale, "Iraqi Pipeline Attacks Go Unreported," United Press International, 27 April 2004: [http://www.upi.com/view.cfm?StoryID=20040427-100003-8797r.](http://www.upi.com/view.cfm?StoryID=20040427-100003-8797r;); Karl Vick, "The Critical Battle for Iraq's Energy," *The Washington Post*, 15 January 2005.
- ²⁰ Karl Vick, "The Critical Battle for Iraq's Energy."
- ²¹ *Financial Times* [London], 19 December 2004.
- ²² Fouad Hussein, *Al-Zarqawi-al-Qaeda's Second Generation* (Paris, 2005), in Arabic; quoted in Yassin Musharbash, "What al-Qaida Really Wants," *Der Spiegel*, 12 August 2005.
- ²³ *Energy in the Americas*, U.S. Department of Energy, Energy Infrastructure Administration, URL: <http://www.worldenergy.org/wec-geis/edc/> (accessed 12 November 2005).
- ²⁴ Natural Resources Canada, Energy Protection Division, *Canada's Energy Systems* (May 2003).
- ²⁵ Statistics Canada, *Canadian Statistics > Primary Industries*, "Gross Domestic Product at Basic Prices, Primary Industries": <http://statcan.ca/english/Pgdb03.htm> (as at 4 February 2005).
- ²⁶ Natural Resources Canada, Energy Policy Branch, Energy Sector, *Canada's Energy Policies—Sustainable Development*. http://www.nrcan.gc.ca/es/epb/eng/sustainable_e.htm (accessed 21 March 2005).
- ²⁷ Asia Pacific Economic Cooperation (APEC), *APEC Energy Statistics 2002* (Energy Working Group, November, 2004), Table: "Energy Balance Table of Canada in 2002," pp. 48–49.
- ²⁸ Statistics Canada, *Canadian Statistics > International Trade*, "Exports of Goods on a Balance-of-Payments Basis": <http://statcan.ca/english/Pgblec04.htm> (as at 4 February 2005).
- ²⁹ In April 2001, Canada, Mexico, and the United States established a North American Energy Working Group to enhance energy trade within the common economic space, and to foster cooperation in hemispheric energy issues, infrastructure, and technologies: North American Energy Working Group, *North America—The Energy Picture* (June 2002).
- ³⁰ "Canada Country Analysis Brief," *EIA Country Analysis Briefs—North America*, U.S. Department of Energy, Energy Information Administration, URL: <http://www.eia.doe.gov/emeu/cabs/canada.html> (accessed 11 November 2005).
- ³¹ "Mexico," *EIA Country Analysis Briefs*, U.S. Department of Energy, Energy Information Administration, URL: <http://www.eia.doe.gov/emeu/cabs/mexico.html> (accessed 12 November 2005).
- ³² "Caribbean Fact Sheet," *EIA Country Analysis Briefs*, U.S. Department of Energy, Energy Information Administration, URL: <http://www.eia.doe.gov/emeu/cabs/carib.html> (accessed 12 November 2005).

- ³³ "United States of America," *EIA Country Analysis Briefs*, U.S. Department of Energy, Energy Information Administration, URL: <http://www.eia.doe.gov/emeu/cabs/usa.html> (accessed 12 November 2005).
- ³⁴ Paul Parfomak, *Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options*, CRS Report for Congress (Washington, DC: Congressional Research, Service 21 December 2005), RL 33206, p. 4.
- ³⁵ Sean Gorman, *Networks, Security and Complexity. The Role of Public Policy in Critical Infrastructure Protection* (Cheltenham, UK/Northampton, MA: Edward Elgar, 2005), p. 82.
- ³⁶ Gal Luft, "Pipeline Sabotage Is Terrorists' Weapon of Choice," *Energy Security*, 28 March 2005.
- ³⁷ See Sean Gorman, *Networks, Security and Complexity*, pp. 45, 78. Paul Parfomak, *Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options*, p. 3. *et passim*.
- ³⁸ Sean Gorman, *Networks, Security and Complexity*, p. 84; Paul Parfomak, *Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options*, p. 9.
- ³⁹ Sean Gorman, *Networks, Security and Complexity*, p. 84.
- ⁴⁰ Cf. United States Department of Defense, *Strategy for Homeland Defense and Civil Support* (Washington, DC: Department of Defense, June 2005), p. 1.
- ⁴¹ Henry Crumpton, "Intelligence and Homeland Defense," in Jennifer Sims and Burton Gerber, eds., *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press, 2005), esp. pp. 202–206.
- ⁴² The Homeland Security Council, David Howe, Senior Director for Response and Planning, *Planning Scenarios. Executive Summaries* (Department of Homeland Security, July 2004), version 2.0.
- ⁴³ Eric Lipton, "U.S. Report Lists Possibilities for Terrorist Attacks and Likely Toll," *The New York Times*, 16 March 2005; Eric Lipton, "Security Chief Signals a Shift in Approach to Terror," *The New York Times*, 17 March 2005.
- ⁴⁴ Canada. Privy Council, *Securing an Open Society: Canada's National Security Policy* (April 2004), p. 7.
- ⁴⁵ *Ibid.*, pp. 22–27.
- ⁴⁶ Cf. *Canadian Security Guide Book, 2005 Edition*, A Report of the Standing Senate Committee on National Security and Defense, First Session, Thirty-Eighth Parliament, December, 2004, esp. Chapter 8.
- ⁴⁷ Henry Crumpton, "Intelligence and Homeland Defense," pp. 213–216.
- ⁴⁸ *Ibid.*
- ⁴⁹ Jacques Shore, "Cooperation. A Legal Imperative?" *FrontLine Defence*, Vol. 2, No. 6 (2005) p. 13.